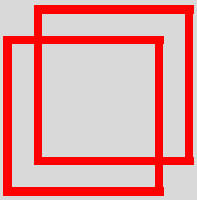
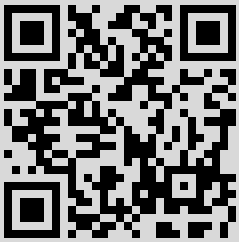


А. Н. Абызов, М. И. Мухаметгалиев, О некоторых матричных аналогах малой теоремы Ферма, *Матем. заметки*, 2017, том 101, выпуск 2, 163–168

DOI: http://dx.doi.org/10.4213/mzm10939



Математические заметки

Том 101 выпуск 2 февраль 2017

УДК 512.552

О некоторых матричных аналогах малой теоремы Ферма

А. Н. Абызов, И. И. Мухаметгалиев

Исследованы кольца, каждая квадратная матрица над которыми представима в виде суммы нильпотентной матрицы и q-потентной матрицы, где q – положительная целая степень простого числа. В качестве следствий получены матричные аналоги малой теоремы Ферма.

Библиография: 7 названий.

Ключевые слова: ниль-чистые кольца, регулярные кольца, малая теорема Ферма.

DOI: 10.4213/mzm10939

1. Введение. Все кольца предполагаются ассоциативными и с единицей. Кольцо называется *чистым*, если любой его элемент является суммой обратимого элемента и идемпотента. Изучение чистых колец было инициировано в работе [1]. Чистые кольца и их обобщения в последнее десятилетие активно изучаются. Кольцо называется *ниль-чистым*, если каждый его элемент является суммой нильпотентного элемента и идемпотента. Всякое ниль-чистое кольцо является чистым. Ряд важных свойств ниль-чистых колец были получены в работе [2]. В этой же работе была поставлена проблема об описании ниль-чистых колец, над которыми кольца матриц также являются ниль-чистыми. В работе [3] была доказана следующая теорема.

Теорема 1. *Для поля P следующие условия равносильны*:
1) *для любого $n \in \mathbb{N}$ кольцо $M_n(P)$ является ниль-чистым*;
2) *для некоторого $n \in \mathbb{N}$ кольцо $M_n(P)$ является ниль-чистым*;
3) $P = F_2$.

Элемент e из кольца R называется *q-потентным*, если для некоторого целого числа $q \geqslant 2$ выполнено равенство $e^q = e$. Кольцо R назовем *q-ниль-чистым*, если каждый элемент из кольца R является суммой нильпотента и q-потентного элемента.

В этой заметке изучаются кольца, над которыми кольца матриц являются q-ниль-чистыми. В качестве следствий доказаны некоторые матричные аналоги малой теоремы Ферма.

2. Основные результаты.

Теорема 2. *Пусть p – простое число, k – целое число $\geqslant 1$, $q = p^k$ и P – поле. Тогда следующие условия равносильны*:
1) *для любого $n \in \mathbb{N}$ кольцо $M_n(P)$ является q-ниль-чистым*;

2) *для некоторого* $m \in \mathbb{N}$ *кольцо* $M_m(P)$ *является* q*-нильь-чистым*;
3) P *– конечное поле и* $|P| - 1$ *делит* $q - 1$.

Доказательство. 1) $\Rightarrow$ 2). Очевидно.

2) $\Rightarrow$ 3). Достаточно показать, что каждый элемент x из поля P удовлетворяет равенству $x^q = x$. Рассмотрим диагональную $(m \times m)$-матрицу A вида $\operatorname{diag}(x, \ldots, x)$. Согласно пункту 2) имеет место равенство $A = E + N$, где $E^q = E$ и N – нильпотентная матрица. Без ограничения общности можно считать, что матрица N имеет нормальную жорданову форму. Поскольку $(A - N)^q = A - N$, то имеем равенство $x^q = x$.

3) $\Rightarrow$ 1). Пусть P – конечное поле и $|P| - 1$ делит $q - 1$. Положим $q' = |P|$. Покажем, что любая матрица $A \in M_n(P)$ представима в виде суммы q'-потентной матрицы и нильпотентой матрицы. Так как в кольце $M_n(P)$ всякий q'-потент является q-потентом, то тем самым будет доказано условие 1).

Рассмотрим фробениусову нормальную форму матрицы $A \in M_n(P)$:

$$F_A = F_{A_1} \oplus F_{A_2} \oplus \cdots \oplus F_{A_k},$$

где F_{A_k} – квадратные блоки вида

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

Ясно, что достаточно показать представимость каждого блока F_{A_k} матрицы F_A в виде суммы нильпотентой матрицы и q'-потентной матрицы. Рассмотрим четыре случая.

Случай 1: $a_{n-1} \neq 0$. Представим F_{A_k} в виде суммы E_{A_k} и N_{A_k}, где

$$E_{A_k} = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_{n-1} \end{pmatrix}, \qquad N_{A_k} = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

Это и есть искомое разложение в сумму, так как N_{A_k} – нильпотентная матрица, $E_{A_k}^{q'} = E_{A_k}$ в силу того, что $-a_i(-a_{n-1})^{q'-1} = -a_i$ в P.

Случай 2: $a_{n-1} = 0$ и $p \neq 2$. Представим F_{A_k} в виде суммы E_{A_k} и N_{A_k}, где

$$E_{A_k} = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 0 & 0 & \ldots & 0 & 0 & -a_1 \\ 0 & 0 & \ldots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & -a_{n-3} \\ 0 & 0 & \ldots & 0 & 1 & -a_{n-2}+1 \\ 0 & 0 & \ldots & 0 & 0 & -1 \end{pmatrix}, \qquad N_{A_k} = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & -1 & -1 \\ 0 & 0 & \ldots & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Матрица N_{A_k} нильпотентная. Так как $E_{A_k}^3 = E_{A_k}$, то $E_{A_k}^t = E_{A_k}$ для любого нечетного натурального t.

Случай 3: $a_{n-1} = 0$, $a_{n-2} \neq 0$ и $p = 2$. Пусть $\phi\colon P \to P$ – автоморфизм Фробениуса, действующий по правилу $\phi(x) = x^2$. В поле P существует элемент z такой, что $z^2 = \phi(z) = a_{n-2}$. Представим F_{A_k} в виде суммы E_{A_k} и N_{A_k}, где

$$E_{A_k} = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 0 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 0 & \dots & 0 & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & a_{n-3} \\ 0 & 0 & \dots & 0 & z & 0 \\ 0 & 0 & \dots & 0 & 0 & z \end{pmatrix}, \qquad N_{A_k} = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & z & a_{n-2} \\ 0 & 0 & \dots & 0 & 0 & 1 & z \end{pmatrix}.$$

Так как $\mathrm{char}(P) = 2$ и для любого $x \in P \setminus \{0\}$ имеет место равенство $x^{q'-1} = 1$, то $E_{A_k}^{q'} = E_{A_k}$ и N_{A_k} – нильпотентная матрица.

Случай 4: $a_{n-1} = 0$, $a_{n-2} = 0$ и $p = 2$. Представим F_{A_k} в виде суммы E_{A_k} и N_{A_k}, где

$$E_{A_k} = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 0 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 0 & \dots & 0 & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 & a_{n-3}+1 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}, \qquad N_{A_k} = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Имеем $E_{A_k}^2 = E_{A_k}$ и N_{A_k} – нильпотентная матрица. Теорема доказана.

Следствие 1. *Пусть R – коммутативное кольцо и I – максимальный идеал кольца R. Если $|R/I| < \infty$, то для всякой матрицы $A \in M_n(R)$ существуют матрицы $E, N \in M_n(R)$ и $m \in \mathbb{N}$ такие, что*

$$A \equiv E + N \pmod{I}, \qquad E^{|R/I|} \equiv E \pmod{I}, \qquad N^m \equiv 0 \pmod{I}.$$

Заметим, что если в следствии 1 положить $R = \mathbb{Z}$ и $n = 1$, то мы получим формулировку малой теоремы Ферма. Следующее утверждение в случае, когда $R = \mathbb{Z}$, было установлено в работе [4].

Следствие 2. *Пусть R – коммутативное кольцо и I – максимальный идеал кольца R. Если $|R/I| < \infty$, то для всякой матрицы $A \in M_n(R)$ имеет место сравнение*

$$\mathrm{tr}(A^{|R/I|}) \equiv (\mathrm{tr}\, A)^{|R/I|} \pmod{I}.$$

Доказательство. Пусть $q = |R/I|$ и $\phi\colon R \to R/I$ – естественный гомоморфизм. Гомоморфизм ϕ индуцирует гомоморфизм $\phi'\colon M_n(R) \to M_n(R/I)$. Тогда согласно следствию 1 имеет место равенство $\phi'(A) = E + N$, где E – q-потентная матрица

и N – нильпотентная матрица. Следовательно, $\operatorname{tr}(\phi'(A)) = \operatorname{tr}(E)$. Из [5; лемма 2.3.1] следуют равенства

$$\phi'(A)^q = (E+N)^q = E^q + N^q + B,$$

где $B \in [M_n(R/I), M_n(R/I)]$. Таким образом,

$$\operatorname{tr}(\phi'(A)) = \operatorname{tr}(E) = \operatorname{tr}(E^q + N^q + B) = \operatorname{tr}(\phi'(A)^q).$$

Следствие доказано.

Кольцо R называется *регулярным* (*по фон Нейману*), если $r \in rRr$ для любого элемента $r \in R$.

Теорема 3. *Пусть p – простое число, k – целое число $\geqslant 1$, $q = p^k$ и R – регулярное коммутативное кольцо. Тогда следующие условия равносильны*:

1) *для любого $n \in \mathbb{N}$ кольцо $M_n(R)$ является q-ниль-чистым*;
2) *для некоторого $m \in \mathbb{N}$ кольцо $M_m(R)$ является q-ниль-чистым*;
3) *в кольце R выполнено тождество $x^q = x$.*

Доказательство. 1) $\Rightarrow$ 2). Очевидно.

2) $\Rightarrow$ 3). Пусть $x \in R$. Рассмотрим диагональную $(m \times m)$-матрицу A вида $\operatorname{diag}(x, \dots, x)$. Согласно пункту 2) имеет место равенство $A = E + N$, где $E^q = E$ и N – нильпотентная матрица. Согласно [6; теорема 1.7] $M_m(R)$ – регулярная R-алгебра. Тогда из [7; теорема 4.10.2] следует существование идеалов $I_1, \dots, I_k$ кольца R и матрицы $B \in M_m(R)$ таких, что имеет место изоморфизм

$$\phi\colon R[N,B] \to \prod_{i=1}^{k} M_{m_i}(R/I_i)$$

R-алгебр, действующий из подалгебры алгебры $M_m(R)$, порожденной матрицами N, B, в прямое произведение алгебр $M_{m_1}(R/I_1), \dots, M_{m_k}(R/I_k)$, выполнены равенства $\bigcap_{i=1}^{k} I_i = 0$, $NBN = N$, $BNB = B$ и $\phi(N) = (J_1, \dots J_k)$, где

$$J_i = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Поскольку $(\phi(A) - \phi(N))^q = \phi(A) - \phi(N)$, то для каждого $1 \leqslant i \leqslant k$ в кольце R/I_i имеет место равенство $(x + I_i)^q = x + I_i$. Так как $\bigcap_{i=1}^{k} I_i = 0$, то $x^q = x$.

3) $\Rightarrow$ 1). Пусть n – призвольное натуральное число и $A \in M_n(R)$. Рассмотрим подкольцо S кольца R, порожденное компонентами матрицы A. Ясно, что S – конечное кольцо и, следовательно, имеет место изоморфизм $S \cong P_1 \times \dots \times P_m$, где P_i – конечное поле и $|P_i| - 1$ делит $q - 1$ для каждого $1 \leqslant i \leqslant m$. Тогда импликация следует из теоремы 1. Теорема доказана.

Импликация 1) $\Rightarrow$ 2) из следующего утверждения была установлена в работе [3].

Следствие 3. *Для коммутативного регулярного кольца R следующие условия равносильны*:

1) *R – булево кольцо*;
2) *R – ниль-чистое кольцо*.

Замечание. Предыдущие два утверждения остаются верными, если в их условиях предположить, что R – полупримитивное коммутативное кольцо. Для этого при доказательстве импликации из 2) в 3) теоремы 3 необходимо воспользоваться теоремой 2 и тем фактом, что каждое полупримитивное коммутативное кольцо является подпрямым произведением полей.

Лемма 1. *Пусть p – простое число и R – p-ниль-чистое кольцо. Тогда имеют место следующие утверждения*:

1) *для любого $n \in \mathbb{N}$ кольцо вычетов Z_{p^n} является p-ниль-чистым*;
2) *если I – идеал кольца R, то R/I – p-ниль-чистое кольцо*;
3) *$J(R)$ – ниль-идеал*;
4) *если R – коммутативное кольцо, то для некоторого целого числа $n \geqslant 1$ выполнено равенство $p^n 1_R = 0$.*

Доказательство. Утверждения пунктов 1) и 2) проверяются непосредственно.

3) Пусть $j \in J(R)$. Для некоторого q-потента e и некоторого целого числа $n \geqslant 2$ выполнены равенства

$$(j-e)^n = 0, \qquad e^n = e.$$

Следовательно, $e \in J(R)$. Таким образом, $e = 0$ и j – нильпотентный элемент.

4) Без ограничения общности можно считать, что R – ненулевое кольцо. Из пункта 3) следует, что в кольце $R/J(R)$ выполнено тождество $x^p = x$. Тогда $p1_{R/J(R)} = 0$, следовательно, существует наименьшее целое число $m \geqslant 2$, для которого выполнено равенство $m1_R = 0$. Если p' – простое число, отличное от p и p', – делит m, то имеет место изоморфизм $R \cong R_1 \times R_2$, где R_1, R_2 – ненулевые кольца и $p'^k 1_{R_2} = 0$ для некоторого $k \in \mathbb{N}$. Тогда в кольце $R_2/J(R_2)$ выполнены равенства $p1_{R_2/J(R_2)} = p'^k 1_{R_2/J(R_2)} = 0$, что невозможно. Таким образом, для некоторого целого числа $n \geqslant 1$ выполнено равенство $p^n 1_R = 0$. Лемма доказана.

Теорема 4. *Пусть p – простое число и R – коммутативное p-ниль-чистое кольцо. Тогда для любого $n \in \mathbb{N}$ кольцо $M_n(R)$ является p-ниль-чистым.*

Доказательство. Пусть $A \in M_n(R)$. Рассмотрим естественный гомоморфизм $\phi\colon R \to R/J(R)$. Гомоморфизм ϕ индуцирует гомоморфизм колец $\overline{\phi}\colon M_n(R) \to M_n(R/J(R))$. Согласно лемме 1,3) в кольце $R/J(R)$ выполнено тождество $x^p = x$. Тогда из теоремы 3 следует равенство

$$\overline{\phi}(A) = E + N,$$

где $E^p = E$ и N – нильпотентная матрица. Ясно, что $R/J(R)$ – подпрямое произведение полей, каждое из которых изоморфно полю F_p. Следовательно, кольцо $M_n(R/J(R))$ можно рассматривать как алгебру над полем F_p. Так как $x^p - x$ – сепарабельный многочлен, F_p – поле разложения этого многочлена и $E^p - E = 0$, то подалгебра $F_p[E]$ F_p-алгебры $M_n(R/J(R))$, порожденная матрицей E, изоморфна конечному прямому произведению поля F_p. Следовательно, для некоторых целых

чисел $1 \leqslant \alpha_1, \ldots, \alpha_k \leqslant p-1$ и попарно ортогональных идемпотентов $f_1, \ldots, f_k \in M_n(R/J(R))$ выполнено равенство

$$E = f_1\alpha_1 + \cdots + f_k\alpha_k.$$

Поскольку согласно лемме 1, 3) $J(R)$ – ниль-идеал, то $\mathrm{Ker}(\overline{\phi}) = M_n(J(R))$ – ниль-идеал. Тогда из [5; лемма 2.3.7] следует существование попарно ортогональных идемпотентов $e_1, \ldots, e_k \in M_n(R)$ таких, что $\overline{\phi}(e_i) = f_i$ для каждого $1 \leqslant i \leqslant k$. Из леммы 1 следует существование целых чисел $\beta_1, \ldots, \beta_k$, для которых выполнены следующие условия: $\beta_i 1_{M_n(R)}$ – p-потентный элемент и $\alpha_i 1_{M_n(R)} - \beta_i 1_{M_n(R)}$ – нильпотентный элемент. Тогда $E' = e_1\beta_1 + \cdots + e_k\beta_k$ – p-потентный элемент и $\overline{\phi}(E') = E$; следовательно, $(A - E')^m \in M(J(R))$ для некоторого целого числа $m \geqslant 1$. Так как $M(J(R))$ – ниль-идеал, то $A - E'$ – нильпотентная матрица. Теорема доказана.

Следствие 4 [3]. *Если R – коммутативное нильь-чистое кольцо, то для любого $n \in \mathbb{N}$ кольцо $M_n(R)$ является нильь-чистым.*

3. Некоторые открытые проблемы.

Задача 1. *Описать все кольца R, над которыми кольца матриц являются q-ниль-чистыми, где q – степень простого числа. Представляет интерес частный случай этой проблемы, когда R – регулярное кольцо.*

Задача 2. *Верно ли, что если над телом T для некоторого $n \geqslant 2$ кольцо $M_n(T)$ является q-ниль-чистым, где q – степень простого числа, то T – поле.*

Авторы искренне признательны рецензенту за внимательное чтение статьи и ряд полезных замечаний, которые значительно улучшили первоначальную версию.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] W. K. Nicholson, "Lifting idempotents and exchange rings", *Trans. Amer. Math. Soc.*, **229** (1977), 269–278.
[2] A. J. Diesl, "Nil clean rings", *J. Algebra*, **383** (2013), 197–211.
[3] S. Breaz, G. Călugăreanu, P. Danchev, T. Micu, "Nil-clean matrix rings", *Linear Algebra Appl.*, **439**:10 (2013), 3115–3119.
[4] В. И. Арнольд, "Динамика Ферма, арифметика матриц, конечная окружность и конечная плоскость Лобачевского", *Функц. анализ и его прил.*, **38**:1 (2004), 1–15.
[5] D. S. Passman, *The Algebraic Structure of Group Rings*, Robert E. Krieger Publ., Melbourne, FL, 1985.
[6] K. R. Goodearl, *Von Neumann Regular Rings*, Monogr. Stud. in Math., **4**, Pitman, Boston, MA, 1979.
[7] K. C. O'Meara, J. Clark, C. I. Vinsonhaler, *Advanced Topics in Linear Algebra. Weaving Matrix Problems Through the Weyr Form*, Oxford Univ. Press, Oxford, 2011.

А. Н. Абызов
Казанский (Приволжский) федеральный университет
E-mail: aabyzov@kpfu.ru

И. И. Мухаметгалиев
Казанский (Приволжский) федеральный университет
E-mail: ilnur.muhametgal@mail.ru

Поступило
12.10.2015